

ABSTRACT OF THE DISCLOSURE

An apparatus and method for performing a modular operation $S=AB \bmod N$, the apparatus arranged such that the constant J_0 , which is ordinarily required in order to complete the operation, is not required to be explicitly computed, thus simplifying and speeding up the operation.

851663.467 / 470114_1.DOC